⑲日本国特許庁(JP)　⑪特許出願公開
⑫公開特許公報(A)　昭63-225839

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和63年(1988)9月20日
G 06 F 12/14	320	B-7737-5B	

審査請求　未請求　発明の数 1　(全3頁)

㊹発明の名称　セキュリティ機能付きROM

㉑特　願　昭62-59463
㉒出　願　昭62(1987)3月13日

㉒発明者　渡邉　修　宮城県仙台市一番町2丁目2番13号　富士通東北デイジタル・テクノロジ株式会社内
㉑出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地
㉔代理人　弁理士　井桁　貞一

明　細　書

1．発明の名称

セキュリティ機能付きROM

2．特許請求の範囲

データを記憶するメモリセル部(3)と、
鍵となるパターンを記憶する鍵パターン記憶部(4)と、
該鍵パターン記憶部の出力と該データを読み出す際に入力された鍵パターンとを照合して，不一致なら該メモリセル部に加えるアドレスを攪乱するアドレス攪乱部(5)とを有することを特徴とするセキュリティ機能付きROM。

3．発明の詳細な説明

〔概要〕

セキュリティ機能付きROMにおいて、ROMの鍵パターン記憶部に記憶された鍵パターンと新たに入力した鍵パターンとを照合して、不一致の時には入力アドレスを攪乱して誤ったデータを読み出す様にして、回路規模を大幅に変更することなく簡単にセキュリティ機能を付加したものである。

〔産業上の利用分野〕

本発明はセキュリティ機能付きROMに関するものである。

ROMは多くの電子機器に使用されているが、セキュリティ機能が付加されているものは殆どないので、これに伴って近年，ROMデータをコピーして使用するデータ盗用が増加している。

そこで、回路規模を大幅に変更することなく簡単に，しかも高性能なセキュリティ機能が付加されたROMが必要である。

〔従来の技術〕

第3図は従来例のブロック図を示す。

以下，コントローラ2内のROMには，鍵になるパターンが書き込まれているとして図の動作を説明する。

先ず、利用者が外部 ROM 1 からデータを読み出す為に鍵パターンをコントロー[redacted]に入力すると、ここに記憶されている鍵パターンと入力された鍵パターンとが比較されるが、不一致の場合には外部ROM 1 内のメモリセルから読み出したデータを入出力コントローラで撹乱してコントローラ 2 を介して出力したり、又はコントローラから入出力コントローラを制御してデータの読み出しを禁止する。

この為、データの解読が不可能になる。

〔発明が解決しようとする問題点〕

しかし、セキュリティ機能を維持する為に専用コントローラが必要となり回路規模が大きくなると云う問題点がある。

〔問題点を解決する為の手段〕

上記の問題点は第 1 図に示すセキュリティ機能付きROM により解決される。

ここで、3 はデータを記憶するメモリセル部で、4 は鍵となるパターンを記憶する鍵パターン記憶部であり、5 は鍵パターン[redacted]部の出力と該データを読み出す際に入力された鍵パターンとを照合して、不一致なら該メモリセル部に加えるアドレスを撹乱するアドレス撹乱部である。

〔作用〕

本発明は読み出されたデータを撹乱するのではなく、読み出しアドレス自体を撹乱して誤ったデータを読み出して、データ盗用が行われない様にする。

即ち、予め鍵パターン記憶部 4 に書き込まれた鍵パターンと入力された鍵パターンとをアドレス撹乱部 5 で比較する。

この時、2 つのパターンが一致すれば、データを読み出す為に入力されたアドレスは撹乱されずにメモリセルに加えられて正しいデータが読み出される。

しかし、不一致の場合には上記のアドレスは撹乱され、撹乱されたアドレスに対応したデータが読み出されるので解読は不可能である。

即ち、ROM 内の鍵パターン記憶部 4 で鍵パターンを記憶することにより、専用コントローラが不要となり、回路規模が縮小する。

〔実施例〕

第 2 図は本発明の実施例のブロック図である。

ここで、出力イネーブル／チップイネーブル回路31，データ入力バッファ32，アドレスデコーダ33，出力バッファ34，メモリセル35，データバス36，アドレスバス37はメモリセル部 3 の構成部分、論理回路51，52，比較論理メモリ53はアドレス撹乱部5 の構成部分を示す。

以下，論理回路51，52はEX-OR ゲートで構成するとして図により動作を説明する。

先ず、出力イネーブル／チップイネーブル回路31にそれぞれ定められた状態の出力イネーブルOE，チップイネーブルCE，制御信号CONT（ 以下，OE，CE，CONT と省略する）と加えてROM を書き込みモードにする。

そして、データをデータバス36，データ入力バッファ32を介してメモリセル部35に書き込んだ後、鍵パターンであるランダムパターンをデータバス，データバッファを介して鍵パターン記憶部41に書き込む。

しかし、このままでは比較論理メモリ53が＂オール 0 ＂になっているので、アドレスが入力すれば対応するデータが読み出される。そこで、これを防止する為にデータバス36，データ入力バッファ32を介してEX-OR ゲート52に＂ 0 ＂を加えて比較論理メモリ53にランダムパターンを書き込む。

次に、出力イネーブル／チップイネーブル回路31に別の状態のOE，CE，CONTを加えてROM を読み出しモードにする。そして、データバス36，データ入力バッファ32を介してランダムパターンをEX-OR ゲート52に加える。ここには記憶されたランダムパターンも加えられているので、2 つのパターンが比較され，一致していれば＂オール 0 ＂が、不一致なら＂オール 0 ＂と異なるパターンが不揮発性メモリで構成された比較論理メモリ53に加え

られる。

一方、アドレスバス37，アドレスデコーダ33を介して入力したアドレスはEX-OR ゲート51に加えられるが、一致の時は"オール0"の為にそのままここを通過し、メモリセルから正しいデータが読み出され，出力バッファ34を介して取り出される。

しかし、"オール0"と異なるパターンの時は入力したアドレスは撹乱されて間違ったアドレスとなる。この為、間違ったデータが出力されるので解読が不可能である。

ここで、上記のランダムパターンを多数バイトにわたって設定したり，このパターンを記憶する領域を任意の場所に設定する様にすれば更にセキュリティの強度が増す。

又、論理回路52の位置をメモリセル35の前段に設けたり，出力バッファ34の前段や後段に設けてもよい。更に、この回路52の構成として例えばより複雑な構成にすることも可能である。

即ち、ROM 単体でセキュリティ機能を持つので、ROM ごとに異なるランダムパターンを入力れば個別にセキュリティを行うことができると共に、専用コントローラを使用しないので回路規模が縮小される。

〔発明の効果〕

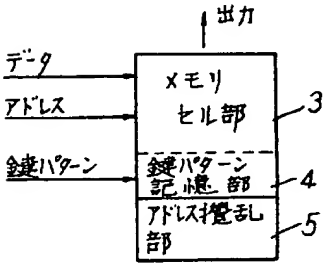
以上詳細に説明した様に本発明によれば、回路規模が縮小されると云う効果がある。

4．図面の簡単な説明

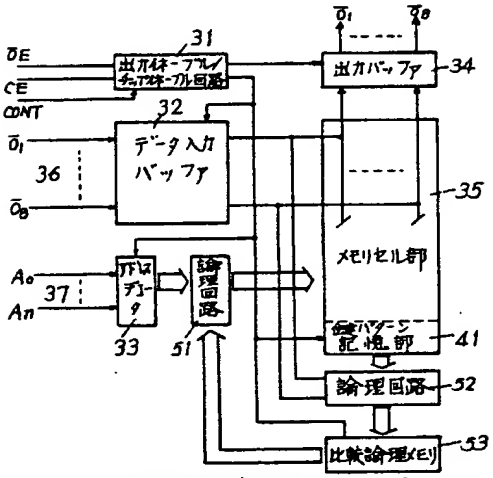
第1図は本発明の原理ブロック図、
第2図は本発明の実施例のブロック図、
第3図は従来例のブロック図を示す。

図において、
3はメモリセル部、
4は鍵パターン記憶部、
5はアドレス撹乱部を示す。

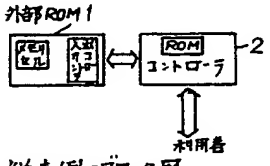
代理人　弁理士　井桁　貞一



本発明の原理ブロック図
第1図



本発明の実施例のブロック図
第2図



従来例のブロック図
第3図